ABSTRACT

Strengthening Crypto-1 Cipher on RFID Tag Against Algebraic Attack
Farah Afianti

Supervisor: Ari M. Barmawi, Ph.D

Crypto-1 is widely used in encryption algorithm especially on RFID tag. However, it has been broken by SAT Solver algebraic attack which has the lowest complexity. In order to strengthen Crypto-1 against SAT Solver, the modification of feedback boolean function which has better cryptographic properties is proposed. It applies primitive polynomial companion matrix [22], Factorization and Common Subexpression Elimination (CSE) [12] optimization concept. The Feedback Shift Register which uses modified Feedback Boolean Function and original Filter Function can not be attacked directly by SAT Solver. It has to be split into small groups. The experiment show that the time to attack the Feedback Shift Register Equation is higher than the time to encrypt the message using those modified Crypto-1. Furthermore, the time to attack the modified Crypto-1 is higher than the original Crypto-1.

Keywords: Crypto-1, RFID, Algebraic Attack, Cryptographic Properties.